# Teorie čísel a úvod do šifrování

RNDr. Zbyněk Šír, Ph.D.

Kurz vznikl v rámci projektu "Rozvoj systému vzdělávacích příležitostí pro nadané žáky a studenty v přírodních vědách a matematice s využitím online prostředí", Operační program Praha – Adaptabilita, registrační číslo CZ.2.17/3.1.00/31165.


Projekt A-NET je financován Evropským sociálním fondem, rozpočtem ČR a MHMP.

"Praha & EU: Investujeme do vaší budoucnosti.

# Teorie čísel a úvod do šifrování

RNDr. Zbyněk Šír, Ph.D.

**Abstrakt**

Tento kurz je věnován teorii dělitelnosti celých čísel a jejím aplikacím pro šifrování. Po úvodní motivaci zadefinujeme relaci kongruence a bude studovat její základní vlastnosti. Kongruence jsou hlavním nástrojem pro studium dělitelnosti. Budeme řešit vybrané rovnice v kongruencích. Na závěr se seznámíme s RSA šifrovacím algoritmem, který z kongruencí vychází.

## Úvodní motivace

Pokusme se přímo vyřešit následující úlohu.

**Příklad 1** *Dokažte, že* $2010^{2010}+1$ *je dělitelné číslem 13.*

*Řešení.* Můžeme psát

$$2010^{2010}+1=(13\cdot 154+8)^{2010}+1$$

a to má stejný zbytek po dělení číslem 13 jako

$$8^{2010}+1.$$

Opravdu, stačí si představit, že $(13\cdot 154+8)^{2010}$ rozepíšeme podle binomické věty, nebo si jen představíme roznásobení všech 2010 závorek a vidímě, že všechny členy jsou dělitelné 13 kromě posledního $8^{2010}$.

Dále platí

$$8^{2010}+1=64^{1005}+1=(13\cdot 5-1)^{1005}+1$$

a to má stejný zbytek po dělení číslem 13 jako

$$(-1)^{1005}+1=0.$$

Celkově tedy zbytek po dělení $2010^{2010}+1$ číslem 13 je 0 a tvrzení je tedy dokázáno.

□

Všimněte si, že podstatou řešení je to, že se při výpočtu zaměřujeme pouze na zytky, které dostatneme při dělení 13. Jaký násobek 13 se přesně v čísle objevuje nás nezajímá, pouze jeho zbytek. Nyní se podobným způsobem pokuste samostatně vyřešit následující úlohy.

**Úloha 1** *Nalezněte $x$ tak aby $4x + 3$ bylo dělitelné 5.*

**Úloha 2** *Nalezněte $x$ tak aby $3x + 5$ bylo dělitelné 6.*

Jistě jste zjistili, že první úloha řešení má, zatímco druhá nikoliv. Zároveň je zejmé, že jestliže nějaké číslo $x$ první úlohu řeší, pak ji bude řešit i číslo $x+6$, $x-6$ a obecně libovolné číslo tvaru $x+6k$, kde $k$ je jakékoliv celé číslo. U čísla $x$ tedy záleží pouze na jeho zbytku po dělení 6. Tato myšlenka je v teorii dělitelnosti velice obecná a je upřesněna v definici kongruence.

## Definice a základní vlastnosti kongruence

Jestliže nebude řečeno jinak, budeme v tomto kurzu číslem myslet číslo celé $\in \mathbb{Z}$.

**Definice 1** *Řekneme, že číslo $a$ je kongruentní s číslem $b$ modulo přirozené číslo $m$ jesliže $m|(a-b)$, tedy $m$ dělí rozdíl $a-b$, čili existuje číslo $k$ tak že $(a-b) = km$. Jinak řečeno $a$ i $b$ dávají stejný zbytek po dělení číslem $m$. Tento vztah zapíšeme symbolicky*

$$a \equiv b \bmod m.$$

Kupříkladu tedy platí kongruence

$$3 \equiv 13 \bmod 10, \quad 35 \equiv 0 \bmod 7, \quad -23 \equiv 1 \bmod 8$$

a podobně. Modul $m$ jsme pro jednoduchost uvažovali kladný, ale teorii by bylo možno vybudovat i pro záporné moduly. Nezískali bychom však věcně žádnou výhodu, protože zjevně dvě čísla jsou kongruentní modulo $m$ právě tehdy když jsou kongruentní modulo $-m$.

Kongruence má následující tři jednoduché, ale velice důležité vlastnosti.

**Věta 1** *Nechť $a, b, c \in \mathbb{Z}$ a $m \in \mathbb{N}$. Pak*

1. $a \equiv a \bmod m$
2. *Jestliže $a \equiv b \bmod m$, pak i $b \equiv a \bmod m$.*
3. *Jestliže $a \equiv b \bmod m$ a zároveň $b \equiv c \bmod m$, pak i $a \equiv c \bmod m$.*

*Důkaz.* První dvě tvrzení jsou triviální. U třetího z předpokladu víme, že existují čísla $k, l$ tak, že $(a-b) = mk$ a $(b-c) = ml$, z čehož ihned plyne $(a-c) = m(k+l)$.

□

První vlastnost (tzv. reflexivita) říká, že každé číslo je kongruentní samo se sebou. Druhá vlastnost je symetrií kongruence a třetí vlastnost se nazývá symetrie. Dohromady tyto tři vlastnosti znamenají, že kongruence je tzv. relací ekvivalence. Význam tohoto tvrzení je, že všechna celá čísla se pro konkrétní modul $m$ rozpadnou do tříd

(množin), přičemž v každé třídě jsou všechna čísla mezi sebou kongruentní a čísla z různých tříd kongruentní nejsou. Například pro $m = 3$ dostaneme tři třídy:

$$\{\ldots, -12, -9, -6, -3, \mathbf{0}, 3, 6, 9, 12 \ldots\}$$
$$\{\ldots, -11, -8, -5, -2, \mathbf{1}, 4, 7, 10, 13 \ldots\}$$
$$\{\ldots, -10, -7, -4, -1, \mathbf{2}, 5, 8, 11, 14 \ldots\}.$$

Jak jsme již řekli, čísla v každém řádku vzájemně jsou kongruentní modulo 3 a mezi různými řádky kongruentní nejsou. Zároveň vidíme, že z každé třídy můžeme vybrat jednoho zástupce (číslo vytištěné tučně), který celou třídu reprezentuje, neboť je právě zbytkem, který dostaneme, když libovolné číslo z dané třídy dělíme číslem 3. V našem případě se jedná o zbytku $0, 1, 2$, v obecném případě jsou to čísla

$$0, 1, \ldots, (m-2), (m-1).$$

Na závěr této kapitoly si ještě zformulujeme větu, která nám říká, že (v mnoha případech) můžeme stejně dobře počítat s libovolným číslem v dané třídě (a kdykoliv libovolné číslo nahradit jiným číslem ve stejné třídě).

**Věta 2** *Nechť $a, b, c, d \in \mathbb{Z}$ a $r, m \in \mathbb{N}$ a platí*

$$a \equiv b \bmod m, \qquad c \equiv d \bmod m.$$

*Pak platí i*

1. $a + c \equiv b + d \bmod m$
2. $a - c \equiv b - d \bmod m$
3. $ac \equiv bd \bmod m$
4. $a^r \equiv c^r \bmod m$

*Důkaz.* Z předpokladu věty víme, že existují čísla $k, l$ tak, že $(a-b) = mk$ a $(c-d) = ml$, z čehož plyne $(a + c) - (b + d) = m(k + l)$, čímž je dokázán bod 1. Podobně $(a-c)-(b-d) = m(k-l)$, čímž je dokázán bod 2. K důkazu bodu 3 si stačí rozepsat

$$ac - bd = (a - b)c + (c - d)b = m(kc + lb).$$

Konečně bod 4 dostaneme $r$ zopakováním bodu 3, přičemž předpokládáme $c = a$ a $b = d$.

□

V dalších kapitolách uvidíme, jak se tato jednoduchá pravidla užívají při řešení konkrétních příkladů. Nyní si ale uveďme dvě odstrašující ukázky toho, která pravidla neplatí. Především není možno dělit; máme sice

$$2 \equiv 6 \bmod 4,$$

ale přitom po vydělení obou stran rovnice 2 dostáváme

$$1 \equiv 3 \bmod 4,$$

což neplatí. Bystrý student si povšimne, že bychom platnou kongruenci dostali, kdybychom i modul 4 vydělili 2. Takové pravidlo by bylo možno sformulovat, ale v našem kurzu se omezíme pouze vždy na počítání v rámci jednoho povného modulu.

Druhou neplatnou úpravou je mocnění na kongruentní exponent. Máme například

$$2^5 = 32 \equiv 2 \bmod 3.$$

Exponent 5 nesmíme nahradit číslem 2, přestože je s 5 kongruentní modulo 3. Dostali bychom totiž $2^2 = 4$, které je kongruentní s 1 a nikoliv 2 modulo 3. Správné zacházení s exponenty je velice důležité (například k efektivnímu řešení úloh podobných naší první motivační úloze). Později si ho vyjasníme sformulováním malé Fermatovy a Eulerovy věty.

## Řešení kongruencí s neznámou

Vraťme se k úlohám 1 a 2. Nyní je můžeme sformulovat jako úlohy: řešte následující kongruence:

$$4x \equiv -3 \equiv 2 \bmod 5, \qquad 3y \equiv -5 \equiv 1 \bmod 6.$$

Podle vět 1 a 2 je přitom jasné, že řešením je celá třída vzhledem ke kongruenci, stačí tedy najít jedno řešení - nejlépe zástupce mezi čísli $0, \ldots, m-1$. Je velice užitečné sestavit si tabulku násobení zbytků modulo 5 a 6. V těchto tabulkách vždy

| $*$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

| $*$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Tabulka 1: Tabulka násobení modulo 5 (vlevo) a modulo 6 (vpravo).

vynásobíme příslušná čísla v záhlaví řádku a sloupečku a výsledek zapíšeme modulo $m$. Například v první tabulce máme $2 \cdot 3 = 6$, ale do tabulky zapíšeme 1, které je s ním modulo 5 kongruentní. Tabulky jsou pochopitelně symetrické. Povšimneme si dvou důležitých věcí. Zaprvé násobení nulou je vyjímečné - vždy dostaneme opět 0. Zadruhé obě tabulky se poněkud liší. V případě $m = 5$ jsou všechny ostatní řádky pěkné - přesněji najdeme na každém z nich všechny zbytky a žádný se neopakuje. V případě $m = 6$ mají tuto vlastnost jen řádky 1 a 5. Ostatní jsou pokažené. Je to způsobeno tím, že čísla 2,3,4 jsou soudělná s modulem 6. Ve vysokoškolské matematice řekneme, že zbytky po dělení 5 (a obecně modulo libovolné prvočíslo) tvoří tzv. těleso, zatímco zbytky po dělení 6 (a obecně modulo libovolné složené číslo) těleso netvoří.

Pohledem do 4. řádku první tabulky zjistíme, že řešením kongruence $4x \equiv 2 \bmod 5$ má řešení $x = 3$ a pohledem do 3. řádku druhé tabulky vidíme, že kongruence

$3y \equiv 1 \bmod 6$ žádné řešení nemá. Kdybychom namísto toho chtěli řešit kongruenci $3y \equiv 3 \bmod 6$, měli bychom hned tři řešení: $y = 0, 2, 4$.

Díky pěkným vlastnostem násobení modulo 5 můžeme snadno nahlédnout, že každá lineární kongruence má právě jedno řešení. Představme si kupříkladu že máme řešit obecnou kongruenci

$$4x \equiv a \bmod 5,$$

kde $a$ je libovolné číslo. Z první tabulky vidíme, že $4 \cdot 4 \equiv 1 \bmod 5$. Podle bodu 3 věty 2 můžeme celou kongruenci vynásobit 4 a dostáváme

$$x \equiv 4a \bmod 5,$$

což je řešení. Abychom se vyhnuli problémům sesoudělnými čísly ("špatným"řádkům tabulky), budeme co možná nejvíce pracovat s prvočíselnými moduly, t.j. $m = p$, kde $p$ je prvočíslo.

**Úloha 3** *Sestavte tabulku násobení pro modul $m = 12$ a rozhodněte, pro která $b$ má kongruence $ax \equiv 1 \bmod 12$ řešení.*

Na závěr této kapitoly si ukážeme, jak řešit lineární kongruence pro velké moduly, kde nelze řešení uhodnout (jako jste to zřejmě udělali u úloh 1 a 2), ani nelze sestavovat tabulku, protože by byla příliš rozsáhlá.

**Příklad 2** *Řešte kongruenci*

$$34x \equiv 133 \bmod 211. \tag{1}$$

*Řešení.* Číslo 211 je prvočíslo, proto úloha bude mít právě jedno řešení (přesněji celou třídu řešení, ale právě jedno mezi čísli $0, 1, \ldots, 210$. Využijeme kongruence, která nepochybně platí pro každé $x$:

$$211x \equiv 0 \bmod 211. \tag{2}$$

Nyní $211 = 34 \cdot 6 + 7$. S využitím věty 2 tedy vezmeme šestinásobek kongruence (1), odečteme ho od (2) a dostaneme

$$7x \equiv -798 \equiv 46 \bmod 211. \tag{3}$$

Podobně $34 = 7 \cdot 4 + 6$ a vezmeme čtyřnásobek kongruence (3), odečteme ho od (1) a dostáváme

$$6x \equiv -51 \bmod 211. \tag{4}$$

Konečně odečtením (4) od (3) dostáváme

$$x \equiv 97 \bmod 211. \tag{5}$$

Řešením je tedy $x = 97$ a je snadné provést zkoušku: $34 \cdot 97 = 3298 \equiv 133 \bmod 211$.

□

Tento postup nám unožňuje efektivně řešit kongruence s libovolně velkým prvočíselným (a někdy i neprvočíselným) modulem.

## Rozšířený Eukleidův algoritmus.

Postup v předchozím příkladu zjevně úzce souvisí s Eukleidovým algoritmem. Připomeňme si jeho aplikaci na čísla v jednoduchém příkladu.

**Příklad 3** *Nalezněte největšího společného dělitele čísel* 633 *a* 102.

*Řešení.* Vstupní čísla si napíšeme do dvojice $(633, 102)$. Dále opakovaně aplikujeme krok Eukleidova algoritmu: menší číslo ponecháme a přesuneme ho na první pozici, větší číslo nahradíme zbytkem pod dělení číslem menším a tento zbytek napíšeme na druhou pozici. Po jedné aplikaci tohoto kroku tedy dostáváme $(102, 21)$, protože zbytek po dělení 633 číslem 102 je 21. V dalších krocích pak postupně dostaneme $(21, 18)$, $(18, 3)$, $(3, 0)$, čímž se algoritmus zastaví. Poslední nenulové číslo 3 je největším společným dělitelem čísel 633 a 102.

□

Eukleidův algoritmus je nesmírně efektivní, protože k výsledku konverguje velice rychle. Pokud je výsledkem číslo 1, pak jsou vstupní čísla nesoudělná. Velice užitečný je i Eukleidův algoritmus pro polynomy, protože může pomoci rozložit polynom na součin polynomů nižšího stupně.

Pro účely teorie dělitelnosti je velice užitečná rozšířená verze Eukleidova algoritmu, která souvisí s takzvanou Bezoutovou větou:

**Věta 3** *Pro daná číslo $a, b$ existují čísla $k, l$ taková, že*

$$ab + kl = 1 \tag{6}$$

*právě tehdy, když $a, b$ jsou nesoudělná.*

*Důkaz.* Když jsou čísla $a, b$ soudělná, pak zjevně rovnice (6) nemůže být splněna, protože společný dělitel $a$ a $b$ by musel dělit 1. Pokud jsou $a, b$ nesoudělná, můžeme čísla $k$, $l$ nalézt pomocí zvláštní varianty Eukleidova algoritmu. Vše bude (i v obecnosti) patrné na následujícím konkrétním příkladu. Uvažujme $a = 1435$ a $b = 263$. Jestliže na tato čísla aplikujeme Eukleidův algoritmus, dostaneme postupně čísla, která jsou napsána v posledním sloupečku následující tabulky

| $a\cdot$ | $+$ | $b\cdot$ | $=$ | |
|---|---|---|---|---|
| 1 | | 0 | | 1435 |
| 0 | | 1 | | 263 |
| 1 | | −5 | | 120 |
| −2 | | 11 | | 23 |
| 11 | | −60 | | 5 |
| −46 | | 251 | | 3 |
| 57 | | −311 | | 2 |
| −103 | | 562 | | 1 |

Do tabulky nyní přidáme další dva sloupečky, které sestrojíme následující způsobem. V prvním řádku začneme $1, 0$ a ve druhém $0, 1$ - viz tabulka. Nyní když dělíme 1435

číslem 263 dostaneme 5 a zbytek 120. Od prvního řádku tedy odečteme pětinásobek druhého řádku - tím dostaneme třetí řádek včetně zmíněného 120. Dále od druhého řádku odečteme dvojnásobek třetího, protože 263 děleno 120 dává 2 (se zbytkem 232). Takto pokračujeme až do posledního řádku. Vzniklá čísla v každém řádku mají následující vlastnost: první číslo vynásobeno 1435 plus druhé číslo vynásobeno 263 dává třetí číslo. Platnost tohoto vztahu je jasná, protože triviálně platí v prvním a druhém řádku, a ostatní řádky jsme dostali jen opakováným kombinováním těchto výchozích řádků. Speciálně tedy poslední řádek nám říká, že

$$57 \cdot 1435 + (-311) \cdot 263 = 1.$$

□

**Úloha 4** *Nalezněta celá čísla $a$, $b$ taková, aby $17a - 16b = 5$.*

**Úloha 5** *Nalezněte největšího společného dělitele čísel 371 a 727 a vyjádřete jej jako lineární kombinaci těchto čísel.*

## Fermatova věta a Eulerova věta

Při řešení kongruencí a počítání se zbytky jsme již získali určitou zběhlost. Budeme ale ještě potřebovat určité nástroje pro práci s mocninami. Pro řešení kongruencí, ve kterých se vyskytují mocniny je velice užitečná tzv. malá Fermatova věta a její zobecnění, tzv. Eulerova věta.

**Věta 4 (Malá Fermatova)** *Nechť $p$ je prvočíslo a $a$ číslo, které je s $p$ nesdoudělné. Pak platí*

$$a^{p-1} \equiv 1 \bmod p. \tag{7}$$

*Důkaz.* Uvažujme množinu všech zbytkových tříd kromě nuly

$$\{1, 2, \ldots, (p-2), (p-1)\}. \tag{8}$$

Tvrdím, že množina

$$\{1a, 2a, \ldots, (p-2)a, (p-1)a\} \tag{9}$$

reprezentuje stejnou množinu zbytkových tříd. Skutečně, protože $a$ je nesoudělné s $p$, nemá žádný z těchto součinů zbytek 0. Navíc k $a$ existuje inverzní prvek $a^{-1}$ (takže $aa^{-1} \equiv 1$) a proto mají všechny součiny v (9) různé zbytky. Kdyby totiž $b_1 a \equiv b_2 a$, pak i $b_1 a a^{-1} \equiv b_2 a a^{-1}$ a tedy $b_1 \equiv b_2$. Protože tedy (8) a (9) reprezentují stejné třídy, platí

$$1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv 1a \cdot 2a \cdot \ldots \cdot (p-2)a \cdot (p-1)a \bmod p$$

a po úpravě

$$\begin{aligned} 1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) a^{p-1} \bmod p \\ 1 &\equiv a^{p-1} \bmod p \end{aligned}$$

□

Tato věta má jednoduchý důsledek, který umožňuje do jediné formulace zahrnout i čísla dělitelná $p$.

**Věta 5** *Nechť $p$ je prvočíslo pak pro každé číslo $a$ platí*

$$a^p \equiv a \bmod p.$$

*Důkaz.* Pro $a \equiv 0 \bmod p$ platí rovnost triviálně. Pro osatní čísla ji získáme vynásobením kongruence (7) číslem $a$.

□

S pomocí těchto vět můžeme řešit i obtížné příklady:

**Příklad 4** *Nalezněte nejmenší přirozené číslo $k$ tak, aby výraz*

$$5n^{13} + 13n^5 + 9kn$$

*byl dělitelný číslem 65 pro každé $n$.*

*Řešení.* Výraz má být dělitelný 65, tedy zároveň 13 a 5. S užitím věty 5 můžeme psát.

$$5n^{13} + 13n^5 + 9kn \equiv 5n + 9kn \equiv (5 + 9k)n \bmod 13.$$

Aby dělitelnost platila pro všechna $n$ musí být $5 + 9k$ dělitelné 13, což nastává pro $k \equiv 11 \bmod 13$. Podobně

$$5n^{13} + 13n^5 + 9kn \equiv 13n + 9kn \equiv (13 + 9k)n \bmod 5,$$

což je dělitelné 5 pro $k \equiv 3 \bmod 5$. Nejmenší $k$ splňující obě podmínky je $k = 63$, které je řešením úlohy.

□

Pokud budeme chtět počítat i s jinými moduly než prvočíselnými, budeme potřebovat nějakou analogii Fermatovy věty pro všechna čísla (a ne pouze prvočísla). Tímto zobecněním je Eulerova věta, která používá tzv. Eulerovu funkci.

**Definice 2** *Pro přirozené číslo $n$ definujeme přirozené číslo $\varphi(n)$ jako počet čísel nesoudělných s $n$ a větších než 0 a menších než $n$. Funkci $\varphi : \mathbb{N} \to \mathbb{N}$ nazýváme Eulerova funkce.*

Například tedy máme $\varphi(6) = 2$ protože právě dvě čísla 1 a 5 jsou nesoudělná s 6. Připomeňte si Tabulku 1, ze které je patrná důležitost rozdělení čísel na soudělná a nesoudělná, když počítáme s daným modulem. Pro libovolné prvočíslo $p$ jsou všechna menší čísla nesoudělná a dostáváme $\varphi(p) = p-1$. Obecně se Eulerova funkce vypočítá podle následující věty.

**Věta 6** *Mějme přirozené číslo $n$ a jeho prvočíselný rozklad*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}.$$

*Pak platí*

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}).$$

*Důkaz.* Dosadíme-li za $n$ jeho prvočíselný rozklad, můžeme uvedenou formuli ekvivalentně přepsat jako

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_1^{k_2-1}) \ldots (p_s^{k_s} - p_s^{k_s-1}). \tag{10}$$

Jestliže $n = p^k$ je mocninou prvočísla, pak všechna soudělná čísla $\leq n$ jsou prostě právě násobky $p$, tedy čísla tvaru $p \cdot a$, kde $a$ je přirozené číslo $\leq p^{k-1}$. Takových čísel je $p^{k-1}$ a nesoudělných čísel je tedy $p^k - p^{k-1}$, nebo-li pro tento případ je splněna formule (10).

Důkaz bude dokončen, jestliže ukážeme, že pro dvě nesoudělná čísla $n_1$ a $n_2$ platí

$$\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2).$$

Opět je jednodušší spočítat soudělná čísla. Číslo menší nebo rovno $n_1 \cdot n_2$ je soudělné s $n_1 \cdot n_2$ pokud je soudělné $n_1$ nebo s $n_2$. Čísel menších nebo rovných $n_1 \cdot n_2$ soudělných s $n_1$ je $(n_1 - \varphi(n_1)) \cdot n_2$. Podobně čísel menších nebo rovných $n_1 \cdot n_2$ soudělných s $n_2$ je $(n_2 - \varphi(n_2)) \cdot n_1$. Některá čísla budou soudělná $n_1$, tak s $n_2$ a těch bude $(n_1 - \varphi(n_1))(n_2 - \varphi(n_2))$. Celkově dostáváme

$$\begin{aligned} \varphi(n_1 \cdot n_2) &= n_1 \cdot n_2 - (n_1 - \varphi(n_1)) \cdot n_2 - (n_2 - \varphi(n_2)) \cdot n_1 + (n_1 - \varphi(n_1))(n_2 - \varphi(n_2)) \\ &= \varphi(n_1) \cdot \varphi(n_2). \end{aligned}$$

□

**Věta 7 (Eulerova)** *Nechť $n$ je přirozené číslo a $a$ číslo, které je s $n$ nesdoudělné. Pak platí*

$$a^{\varphi(n)} \equiv 1 \bmod n. \tag{11}$$

*Důkaz.* Důkaz je podobný jako u Fermatovy věty. Jestliže

$$\{b_i\}_{i=1}^{\varphi(n)}$$

je množina všech zbytkových tříd nesoudělných s $n$, pak

$$\{b_i \cdot a\}_{i=1}^{\varphi(n)}$$

je tatáž množina zbytkových tříd. Dále důkaz probíhá analogicky.

□

## RSA šifrovací algoritmus

RSA algoritmus využívá teorie kongruencí pro velmi elegantní šifrování a dešifrování zpráv a dat. Zkratka pochází z iniciál autorů algoritmu, kterými jsou Rivest, Shamir, Adleman. Tento algoritmus má tu vlastnost, že zprávu není možno bez klíče rozluštit, a to i v případě, že víte jakým způsobem byla zakódována. Proto se zcela běžně používá pro bezpečný přenos dat po internetu.

Algoritmus funguje následujícím způsobem.

1. Nalezneme dvě dostatečně velká prvočísla $p$, $q$. V praxi jsou volena čísla délky kolem 384 bitů, tedy kolem 100 cifer v desítkové soustavě. Na ukázku budeme volit nesrovnatelně menší prvočísla $p = 11$ a $q = 13$.
2. Položíme $n = pq$ a tím pro číslo $n$ známe Eulerovu charakteristiku, která je $\varphi(n) = (p-1)(q-1)$. V našem příkladu máme $n = 143$ a $\varphi(n) = 120$. Je zcela zásadní, že pokud $p$, $q$ byla zvolena dostatečně velká a zůstala utajena, pak jejich součit $n$ není možno v rozumném čase rozložit a proto nelze ani spočítat $\varphi(n)$.
3. Zvolíme si tak zvaný veřejný klíč $r$, který je menší než $\varphi(n)$ a je s ním nesoudělný. Dále nalezneme tzv. privátní klíč $s$, který je definován jako řešení kongruence

$$r \cdot s \equiv 1 \bmod \varphi(n). \tag{12}$$

   Tuto kongruenci vyřešíme např. postupem uvedeným na str. 5. V našem příkladu volíme $r = 43$ a dopočítáme $s = 67$. Skutečně platí

$$43 \cdot 67 = 2881 \equiv 1 \bmod 120.$$

4. Zpráva kterou chceme zašifrovat je nějaké číslo $z$ menčí než $n$ a nesoudělné s $n$. Zašifrujeme ho tak, že jej umocníme na veřejný klíč $r$ modulo $n$. Výsledek je šifra $w$. Máme tedy

$$w \equiv z^r \bmod n.$$

   V našem příkladě si zvolíme třeba $z = 50$, které zašifrujeme jako

$$w = 106 \equiv 50^{43} \bmod 143.$$

5. Šifru $w$ opět můžeme rozšifrovat tak, že ji umocníme na privátní klíč $s$ modulo $n$. Tvrdíme tedy, že

$$z \equiv w^s \bmod n.$$

   V našem příkladě skutečně dostáváme

$$106^{67} \equiv 50 \bmod 143.$$

Není obtížné se přesvědčit, že dešifrování funguje opravdu správně. Díky (12) máme $rs = k\varphi(n) + 1$ a tedy podle Eulerovy věty dostáváme

$$w^s \equiv (z^r)^s = z^{k\varphi(n)+1} \equiv (z^{\varphi(n)})^k \cdot z \equiv z \bmod n.$$

Zdůrazněme, že i když víme jak byla zpráva zašifrována, tedy známe $n$, $r$ a výsledek $w$, nejsme schopni nalézt $s$ a tedy ani $s$. Efektivnost algoritmu je založena zejména na tom, že je mnohem lehčí nalézt prvočísla $p$, $q$, než rozložit jejich součin. Je to mu tak proto, že existují pravděpodobnostní testy, které s vysokou pravděpodobností ověří, že dané číslo je prvočíslo.

RSA algoritmus dokreslujeme na dostatečně velkých číslech v příloze na konci kurzu.

## Zajímavé úlohy na závěr

**Úloha 6** *Dokažte, že pro každé přirozené $n$ je číslo*

$$5 \cdot 2^{4n} - 7^{2n+1} - 19 \cdot 10^{2n} + 21^{n+1}$$

*dělitelné* 14.

**Úloha 7 (MO Kanada 1989)** *Transformací čísla rozumíme, že ho nahradíme jeho ciferným součtem v desítkové soustavě. Jaké číslo dostaneme, jestliže opakovaně provedeme čtyřikrát transformaci čísla* $2007^{2007}$ *?*

**Úloha 8 (Prasátko, 24. ročník)** *Pro dané prvočíslo $p$ nalezněte všechna celá čísla $a$, $b$ tak, aby*

$$a^2 \equiv b^3 \bmod p.$$

**Úloha 9 (MO USA 1976)** *Určete všechna celočíselná řešení rovnice*

$$a^2 + b^2 + c^2 = a^2 b^2.$$

**Úloha 10** *Dokažte, že neexistují žádná celá čísla $x$, $y$, tak aby*

$$x^2 - 4y^2 = 246834.$$

**Úloha 11 (MO USA 1979)** *Nalezněte všechna celočíselná řešení $n_1, n_2, \ldots, n_{14}$ rovnice*

$$n_1^4 + n_2^4 + \ldots + n_{14}^4 = 1599.$$

**Úloha 12** *Je číslo*

$$123^{203^{1055}} - 6^{201030102}$$

*dělitelné 43?*

**Úloha 13 (MO Brazílie 1992)** *Dokažte, že existuje přirozené číslo $n$ takové, že prvních 1992 číslic z $n^{1992}$ jsou jedničky.*

## Úlohy k domácímu řešení

**Úloha 14** *Dokažte, že čtvrtá mocnina každého přirozeného čísla je dělitelná pěti beze zbytku nebo se zbytkem 1.*

**Úloha 15** *Dokažte, že* $200^{200} - 1$ *je dělitelné* 13*.*

**Úloha 16** *Nalezněte přirozené číslo* $x$ *tak, aby* $91x$ *dávalo po dělení číslem* 337 *zbytek* 17*.*

**Úloha 17** *Nalezněte nejmenší přirozené číslo, které je zároveň dělitelné číslem* 4 *se zbytkem* 2*, číslem* 5 *se zbytkem* 3 *a číslem* 7 *se zbytkem* 5*.*

**Úloha 18** *Jisté přirozené dvojciferné číslo* $x$ *zašifruji následujícím způsobem pomocí RSA algoritmu: umocním* $x$ *na* 13 *a vezmu zbytek po dělení číslem* 143*. Tento zbytek (šifra) vyšel* 96*. Určete číslo* $x$ *(tedy rozluštěte šifru).*

```
> ##### tento soubor popisuje implementaci RSA algoritmu pro cisla takove
  velikosti,      jaka jsou pouzivana v praxi.
> restart;
> with(StringTools):
Warning, the assigned name Group now has a global binding
>
>
> pismena:=[a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z];for kk
  from 1 to nops(pismena) do pismena[kk]:=convert(pismena[kk], string):od:
```

$$pismena := [a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z]$$

```
> pismena:=[" ", op(pismena)];;
```

$$pismena := [" ", "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"]$$

```
> cisla:=[seq(convert(i+24, string), i=1..nops(pismena))];
```

$$cisla := ["25", "26", "27", "28", "29", "30", "31", "32", "33", "34", "35", "36", "37", "38", "39", "40", "41", "42", "43", "44", "45", "46", "47", "48", "49", "50", "51"]$$

```
> zprava:="toto je uplne ta nejtajnejsi zprava";
  kod:=zprava;
```

$$zprava := "toto je uplne ta nejtajnejsi zprava"$$

$$kod := "toto je uplne ta nejtajnejsi zprava"$$

```
> for i from 1 to nops(pismena) do
    kod:=SubstituteAll(kod, pismena[i], cisla[i]):
  od:
>
> kod;
"4540454025353025464137393025452625393035452635393035443425514143264726"
> ####### tajnou zpravu jsme si jednoduchym zpusovem prevedli na dlouhe
  cislo   - pouze jsme kazde pismeno nahradili dvojcifernym cislem
>
>
>
> kod:=4540454025353025464137393025452625393035452635393035443425514143264
  726;
>
```

$$kod := 4540454025353025464137393025452625393035452635393035443425514143264726$$

```
>
> d:=trunc(log10(2^1024));
```

$$d := 308$$

```
> rra:=rand(10^(d+2)..10^(d+3));
```

```
rra := proc()
local t;
global _seed;
        _seed := irem(a*_seed, p); t := _seed; to concats do
                _seed := irem(a*_seed, p); t := s*t + _seed;
        end do;
        irem(t, divisor) + offset;
end proc;
```

```
> p:=nextprime(rra());q:=nextprime(rra());
```

$$p := 774196690813211106932703436330736974742561435635584587189767467538305380320622220857\backslash$$
$$22974121768604305613921745580037409259811952655310075487163797179490457039169594160\backslash$$
$$08843057167496049883408581292045791645374701946164403139530792062494734995105353008\backslash$$
$$61464863071981555907634664293926737095254285109732726006090 91$$

$$q := 49760099374675982933766845473509473676470788342281338779191792495900393751209539 3006\backslash$$
$$28363443011313746086538005862664913074813656220643842443844131905754565672075358391\backslash$$
$$13553710879599163815547445261087430974286723136050254230838219905367559282524078861\backslash$$
$$39918985672771168817937493408077283357953943012616294798712 13$$

```
> ######### nahodne jsme si vybrali dve dostatecne dlouha prvocisla p, q,
  ktera   musi zustat tajna
```

```
> n:=p*q;
```

$$n := 385241042704106813033803611494574237566808028572472702330760774666396956069708914696\backslash$$
$$33060237970104749868164989720201907514266267630956702608314929399494631850410668622\backslash$$
$$94010665600006104995659011345471236037334872037928621314181322669141156332207913732\backslash$$
$$09618353693611496989279248927564728930035716007965276616217877526761239735799704609\backslash$$
$$35414941545646019900423060537204830893069945385546193389670608055169524653505207606\backslash$$
$$50565564285819292628114611398509354544398316340615274222642035728426306817383094366\backslash$$
$$50229370826260808941810905161847254031535697308689074573146696686698077411442955392\backslash$$
$$60427126882118653529432803031880369973 83$$

```
> phi:=(p-1)*(q-1);
```

$$\varphi := 385241042704106813033803611494574237566808028572472702330760774666396956069708914696\backslash$$
$$33060237970104749868164989720201907514266267630956702608314929399494631850410668622\backslash$$
$$94010665600006104995659011345471236037334872037928621314181322669141156332207913732\backslash$$
$$09618353693611496989279248927564728930035716007965276616217864808784394136090341905\backslash$$
$$63523875713934512631104002139229849207677448076228360672056744541793876854324690601\backslash$$
$$90814121583496958002505735444591423536469231095592562977689484504458626346430957376\backslash$$
$$94202817693038189280385822947189883662523729446394796943714826672859589963915708136\backslash$$
$$88269424878098200321204680682859565170 80$$

```
> ######## soucin n je verejny, ale eulerova charakteristika phi musi
  zustat   tajna
```

```
> verejny:=65537; ### zvolime si verejny kod
```

$$verejny := 65537$$

```
> assign(msolve(verejny*privatni=1, phi));
```

```
> privatni;
```

$$333765451649284905382598670379509669485074993703480477262318946328913730650442836511553 0\backslash$$
$$40314927834306958574258253057709181079188257888150830846955353968780454753462076466\backslash$$
$$61518343584027595635849092246636586946920718614998889057402864616149128395462366056\backslash$$
$$01434719816408906613936266097823923497864554719991191060067418828737819431712376515\backslash$$

```
        381636384334997320727591231626162338717826217627170849111120562516330910105638610775
        598644293997704170584034276669710851462443517014397780198865012375915819078932302015
        010099044369420846708007600960670091852477175178251162134150914700883701014553629555
        182484060020773361615223725172208673
```

```
> ######## privatni kod ziskame resenim rovnice privatni*verejny = 1
  modulo phi, tento kod musi zustat tajny
```

```
>
```

```
>
```

```
> sifra:=kod &^ verejny mod n;
```

```
sifra := 200792434472421568517611701053830935468797590377185285285713146238368347185291542390
        904621384553748516694697539462008726765971495761392677172149382241717952597775436955
        479553347573701792404716310678608135715345564829780710099718743891351198072281929360
        051254469147769015415092444202265198665374394949210393535696779880702844343212259350
        510627690911739874199625799717310019836328512870499384705682802906770790302017068810
        731934585152935039211332985102857696237701632763267793932633072010913128124400172760
        358013631976778750443697327657768784239275098151352765383645575649347135035138448750
        448902987161522772682877312249959551342163
```

```
> ### zasifrujeme zpravu kod tim, ze ji umocnime na verejny kod modulo n
```

```
>
```

```
>
```

```
> kod2:=sifra &^ privatni mod n;
```

```
kod2 := 45404540253530254641373930254526253930354526353930354434255141432647260
```

```
> ### zpravu opet rozsifrujeme tim, ze ji umocnime na privatni kod modulo
  n
```

```
> kod2:=convert(kod2, string);
```

```
kod2 := "45404540253530254641373930254526253930354526353930354434255141432647260"
```

```
> for i from 1 to nops(pismena) do
    kod2:=SubstituteAll(kod2, cisla[i], pismena[i]):
  od:
```

```
> kod2;
```

"toto je uplne ta nejtajnejsi zprava"

```
> ### a na zaver opet cisla prevedeme na pismena
```

```
>
```

```
>
```